REMARKS/ARGUMENTS

Claims 1-8 are pending. In this response, no amendments are made to the claims. Thus, claims 1-8 will remain pending.

In the Office Action, the Examiner rejected all the claims over the cited references. In particular, the Examiner rejected claims 1-5 under 35 USC §102(e) as allegedly being anticipated by U.S. Patent No. 6,490,682 to Vanstone et al. (hereinafter "Vanstone") and rejected claims 6-8 under 35 USC §102(e) as allegedly being anticipated by U.S. Patent No. 6,467,684 to Fite et al. (hereinafter "Fite").

Claims 1-5

Claims 1-5 were rejected as allegedly being anticipated by Vanstone. Applicants respectfully request reconsideration and withdrawal of that rejection, as Vanstone fails to disclose or suggest each element of claim 1, for reasons set forth below.

For Example, Vanstone pertains to a situation where a pair of correspondents has to mutually authenticate each other. For this reason, more than one round-trip is inherently called for. On the other hand, the presently claimed invention is directed to a situation where the client is required to authenticate herself to the server. The presently claimed invention is directed to a technique of employing only one round trip for authentication, where the authenticity of the server is not in question.

In addition, Vanstone points out in col. 1: "The invention relates to a protocol for the secure receipt and transmission of data between a pair of correspondents and in particular for the secure receipt of data by a client in a client-server environment." In stark contrast, the presently claimed invention is pertinent to any general transaction (including online transactions). In Vanstone, before accepting the data from the server, the client has to authenticate the server and hence a single round-trip transaction is not possible, while the presently claimed invention pertains to general situations where a single round trip authentication is called for. As an example, consider online transactions. If a customer wants to buy items

online and if the transaction takes a long time (e.g., with two round trips), the customer may be inclined to walk away without buying the items.

Furthermore, many transactions of interest (such as online transactions) have to be completed expeditiously. Thus, the information sent from one party to the other needs to be as short as possible. In Vanstone, for example, the message from the client to the server has the following items: client identification, public key of the client, a random number, and a signature (of a hash of the prior three values). In contrast, in the presently claimed invention, a shorter message is sent that may include the following items, namely: client identification, challenge, and the signed challenge.

In addition, the scheme of Vanstone suffers from replay attack. Any one who listens to the communication between the client and the server can pretend to be the client. He can send the same message that the client sent again and again and try to authenticate himself to the server. The presently claimed method avoids this problem by forcing the challenge to be different every time an authentication is requested. As set forth in the specification, one way of doing this is to let C be a running index of successive integers. That is, the first time an authentication is requested, C will be 1, the second time it will be 2, and so on. Alternatively, C could be a function of the client's public key, a running index, the client machine's ID, etc. The server has access to the same function as the client and hence it knows what C should be on any given request.

For reasons set forth above, Applicants respectfully submit that claim 1 is patentable over the Vanstone reference. Furthermore, considering that claims 2-5 derive patentability at least from their dependence on claim 1, these claims are also allowable.

Claims 6-8

Claims 6-8 were rejected as allegedly being anticipated by Fite. Applicants respectfully request reconsideration and withdrawal of that rejection, as Fite fails to disclose or suggest each element of claim 6, for reasons set forth below. For example, Fite does not disclose or suggest the generation of a one-time use card number at the user system. There is no mention

of the internet access terminal generating the credit card number. The customer internet access terminal is only meant for enabling the customer to connect to the internet. And hence it is clear that the Fite scheme fails to disclose or suggest the claimed step of generating the one-time use card number at the user system. Applicants note that Fite is completely silent with regard to the generation of a one-time use card number.

In addition, Fite discloses cards that are inactive to begin with until they are activated by the issuer. There is no such concept of activation in the presently claimed invention. The one-time use card number is generated by the user system and sent to the issuer system and the merchant system. The transaction is approved by the issuer system when the numbers received from the merchant and the user match.

Furthermore, the one-time number of the presently claimed invention is such that it resembles a valid credit card number to the merchant system. This is preferable since the merchant system can use the existing payment networks to process the transactions. Since the one-time number is specific to a transaction, an interloper that intercepts the one-time number is prevented from using it for illicit gain. The Fite card has no such properties.

Accordingly, for reasons set forth above, Applicants respectfully submit that claim 6 is patentable over the Fite reference. Furthermore, considering that claims 7-8 derive patentability at least from their dependence on claim 6, these claims are also allowable.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 925-472-5000.

Respectfully submitted,

Babak Kusha

Babak Kusha
Reg. No. 51,095

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 925-472-5000
Fax: 415-576-0300
Attachments
BK:lls
60076230 v1